WHAT IS CLAIMED IS:

1. A method for analyzing database security, said method comprising:
connecting to one or more servers, wherein each server includes an instance, the instance including one or more databases;
selecting one of the databases;
identifying a user id, wherein the user id has access to the selected databases;
retrieving a permitted user id list corresponding to the selected database;
determining whether the user id is included in the permitted user id list;
reporting the user id in response to the determining.

2. The method as described in claim 1 further comprising:
retrieving a resolution corresponding to the determining; and
including the resolution in the reporting.

3. The method as described in claim 1 wherein the determining further comprises:
identifying a violation message type wherein the violation message type is selected from the group consisting of a removed users check, a DB files and logs access check, and a DB backup files and logs access check.

4. The method as described in claim 1 wherein the database is selected from a group consisting of a database, a backup database, and a directory of databases.

5. The method as described in claim 1 wherein the connection is secure.

6. The method as described in claim 1 wherein the permitted user id list is selected from the group consisting of a database instance owner, a sysadm group, and a sysmaint group.

7. The method as described in claim 1 wherein the servers are on different operating platforms.

8. An information handling system comprising:
one or more processors;
a memory accessible by the processors;
one or more nonvolatile storage devices accessible by the processors;
a database analysis tool to analyze database security, the database analysis tool including:
means for connecting to one or more servers, wherein each server includes an instance, the instance including one or more databases;
means for selecting one of the databases;
means for identifying a user id, wherein the user id has access to the selected databases;
means for retrieving a permitted user id list corresponding to the selected database;
means for determining whether the user id is included in the permitted user id list;
means for reporting the user id in response to the determining.

9. The information handling system as described in claim 8 further comprising:

retrieving a resolution corresponding to the determining; and

including the resolution in the reporting.

10. The information handling system as described in claim 8 wherein the determining further comprises:

identifying a violation message type wherein the violation message type is selected from the group consisting of a removed users check, a DB files and logs access check, and a DB backup files and logs access check.

11. The information handling system as described in claim 8 wherein the database is selected from a group consisting of a database, a backup database, and a directory of databases.

12. The information handling system as described in claim 8 wherein the permitted user id list is selected from the group consisting of a database instance owner, a sysadm group, and a sysmaint group.

13. The information handling system as described in claim 8 wherein the servers are on different operating platforms.

14. A computer program product stored in a computer operable media for analyzing database security, said computer program product comprising:

means for connecting to one or more servers, wherein each server includes an instance, the instance including one or more databases;

means for selecting one of the databases;

means for identifying a user id, wherein the user id has access to the selected databases;

means for retrieving a permitted user id list corresponding to the selected database;

means for determining whether the user id is included in the permitted user id list;

means for reporting the user id in response to the determining.

15. The computer program product as described in claim 14 further comprising:

retrieving a resolution corresponding to the determining; and

including the resolution in the reporting.

16. The computer program product as described in claim 14 wherein the determining further comprises:

identifying a violation message type wherein the violation message type is selected from the group consisting of a removed users check, a DB files and logs access check, and a DB backup files and logs access check.

17. The computer program product as described in claim 14 wherein the database is selected from a group consisting of a database, a backup database, and a directory of databases.

18. The computer program product as described in claim 14 wherein the connection is secure.

19. The computer program product as described in claim 14 wherein the permitted user id list is selected from the group consisting of a database instance owner, a sysadm group, and a sysmaint group.

20. The computer program product as described in claim 14 wherein the servers are on different operating platforms.